Hendry County Sheriff's Office

General Order 5.7

TITLE: Information Services	**SHERIFF'S APPROVAL:** Digital
ORIGINATION DATE: August 8, 2018	**REVISION DATE:** May 7, 2019
RELATED REFERENCES: **CFA:** 26.04M, 32.01	
REVIEW FREQUENCY: 3 YEARS	**DATE OF NEXT REVIEW:** May 7, 2022

I. PURPOSE: To establish guidelines on the proper and improper use of equipment and information service provided by the agency.

II. SCOPE: This order shall apply to all sheriff's office members.

III. POLICY:

A. Equipment Movement and Networking

1. Agency personnel are to avoid unnecessary repairs and damages to agency owned computer and network hardware, and to ensure alterations to computer and network hardware are made in accordance with service contracts or warranties.

2. No equipment may be relocated or transferred between units or districts without written authorization or presence of a staff member from the Information Technology Unit (ITU).

B. Electronic Mail

1. The electronic mail system is provided to assist in conducting the business of this agency.

2. Agency personnel shall comply with federal, state and local requirements pertaining to electronic mail as outlined in this Policy.

3. All electronic mail generated on the Sheriff's e-mail server shall be retained according to retention requirements set by the Florida Department of Management Services.

4. Electronic mail must be used in a responsible, ethical, and legal manner. Inappropriate use can result in disciplinary action.

C. Field Mobile Data Computer Issuance Terms and Conditions

1. All users of a mobile data computer, whether issued for individual use or used in a pool car, shall sign an acknowledgement of this policy in PowerDMS prior to using the equipment.

D. Internet

1. Access must be used in a responsible, efficient, ethical, and legal manner. Inappropriate use can result in cancellation of privileges and other possible disciplinary actions.

2. Restrictions: Hendry County Sheriff's Office employees are not permitted to engage in the following activities either during normal or non-working hours, when using Sheriff's Office equipment or facilities, or when using Sheriff's Office Internet Protocol (IP) address. Internet users shall not:

   a. Access, retrieve, or print text and graphics information that exceeds the bounds of generally accepted standards, good tastes, and ethics or in violation of any Sheriff's Office rules and regulations.

   b. Engage in activities that would in any way bring discredit to the Sheriff.

   c. Engage in offering services or merchandise for sale.

   d. Engage in any activity that would compromise the security of any Sheriff's Office host computer.

   e. Intentionally modify files, other data, or passwords belonging to other users, or misrepresent others while using the network.

3. Supervisory Responsibility

   a. The Sheriff or Chief Deputy will have final authority in determining appropriate Internet behavior. Command staff will have the responsibility of acquiring Internet access for their employees whose job performance will be enhanced. Command staff will request Internet access and electronic mail accounts through the Information Technology Unit (ITU).

IV. PROCEDURE

A. Unit Supervisors

1. All unit supervisors should consult with ITU regarding any computer or technological purchase and must receive final approval from ITU.

2. All computer-related consumables (toner, paper, flash drives, etc.) must be included in the individual unit budget.

3. All repairs beyond the warranty period must be budgeted for by the individual unit. (All computer-related equipment is covered by at least a one year parts and labor agreement under the manufacturer's warranty.)

B. Training

1. The Training Unit is responsible for all training of software and hardware, whether internally or through outside entities.

C. All Employees

1. All employees have restricted access set by ITU.

2. Passwords are confidential and should not be shared with anyone. Any violations should be reported to ITU.

3. Do not leave sensitive or confidential information displayed on the monitor when you are not working on the computer.

4. Do not use any external storage media on a workstation before checking it for viruses.

5. Users must LOG OFF the system when leaving a workstation unattended.

6. The Smartcop systems, along with the agency's central records, are backed up daily. The type of back-up procedure implemented is server to server. This automated process occurs during off business hours in order to avoid system overload during peak hours. Computer file maintenance is an on-going process, with system checks completed on a regularly scheduled basis. Retention of computer files will be according to records retention laws.

7. All data stored on any workstation is not backed-up by the network. It is each user's responsibility to back up their data. All equipment will fail at some point and each user should always be prepared for such situations.

8. It is each user's responsibility to maintain a clean workstation and to avoid food or drink damage to it.

9. Any employee requiring a LOGIN or password for the Smartcop system or alterations of existing LOGIN or password must complete an email to their supervisor, he/she will forward the approved request to the Information Technology Unit (ITU).

10. Users shall not install computer software.

11. Termination of employment with Sheriff's Office will be removed from the system within 30 days.

D. Information Technology Unit (ITU)

1. ITU is responsible for all hardware installation, networking and software installation of all computer related equipment as indicated in the work order system.

2. ITU holds all licenses for software installed on agency computers except as authorized.

3. ITU houses and distributes primary office software to Sheriff's Office personnel in the field. Although there are instances where an office or unit requires a unique form of software to perform a specific function, the offices or units using specific software must possess a valid license from the manufacturer. These licenses must be acquired and maintained for each PC that will have the software installed. These specialty licenses may remain on site and will be subject to inspection by ITU personnel.

4. The introduction of external storage media from outside of the agency may contain computer viruses that may damage the host system or PC. All disks and software will be inspected for virus infection prior to introduction into the Sheriff's Office computer system or any PC. All units will ensure that current anti-virus software is installed on agency computers.

5. ITU is responsible for removing and auditing users on an annual review to verify only authorized members have access.

E. Requests for Service

1. All requests for service must be made by submitting the request through ITU email.

F. Requests for Programming Services

1. All requests for programming services for the purpose of the creation of new services or modification of existing services must be submitted via work order to the Information Technology Unit (ITU). Work orders should contain a brief outline of the project, a statement of justification, and benefits to the Sheriff's Office.

2. If a requested project impacts any existing systems then a statement of impact should also be included with the request for service.

3. ITU will review all requests and will meet with the unit supervisor and any other units that may be impacted by the requested project for the purpose of clarification and scheduling.

4. Upon completion of the initial meetings, ITU will assign the project a timeline and a programmer, who will be the primary contact throughout development.

5. In the event that the project is rejected by ITU, the requesting unit and Chief Deputy will be notified in writing via chain of command.

6. Once the project has been assigned, the programmer will contact the requesting unit to coordinate purchase or development and testing.

7. Upon complete deployment, ITU will notify the command staff and provide a brief description of the project.

G. Electronic Mail

1. The Sheriff's Office retains the right to retrieve and read any electronic mail messages. Electronic mail messages are considered public records and subject to FS.119.

2. Employees are not authorized to retrieve or read e-mail messages that are not sent to them or given access to them by the intended recipient. Any exception must receive prior approval by the supervisor.

3. Any employee who discovers a violation of this policy will notify ITU, who will consult with the Chief Deputy to determine the need for submission to Professional Standards Unit.

V. GLOSSARY

COMPUTER EQUIPMENT – Any component which is connected to a personal computer, mainframe or other type of host computer via serial, parallel or network connection. SERIAL -RS-232 communications protocol used by dumb terminals and personal computers emulating a dumb terminal.

ELECTRONIC MAIL (E-MAIL) – Electronic transmission medium for messages, documents, and other forms of correspondence.

INTERNET – Worldwide Network established by the Department of Defense Advanced Research Projects Agency for the purpose of information interchange.

MOBILE DATA COMPUTER – Any laptop computer issued for the purpose of field reporting, data collection or any other field use.

NETWORK – Protocol by which personal workstations are connected to a host server and other workstations within the existing LAN.

Your electronic signature in Power DMS acknowledges you have read this policy and understand it.